Classical Data Representation

- The basic unit in classical data is a binary digit, called a bit, that can take on the value 0 or 1.
- In classical computing, we represent a datum by a string of bits.
- The letter ‘A’ may be written 0100 0001
- The number 137 can be written 1000 1001

Classical Operations

- All operations in classical computing are based on logic gates.
- For example, the logical AND gate takes in two bits and returns 1 if and only if both inputs are 1.

AND		
Input 1	Input B	Output
0	0	0
0	1	0
1	0	0
1	1	1

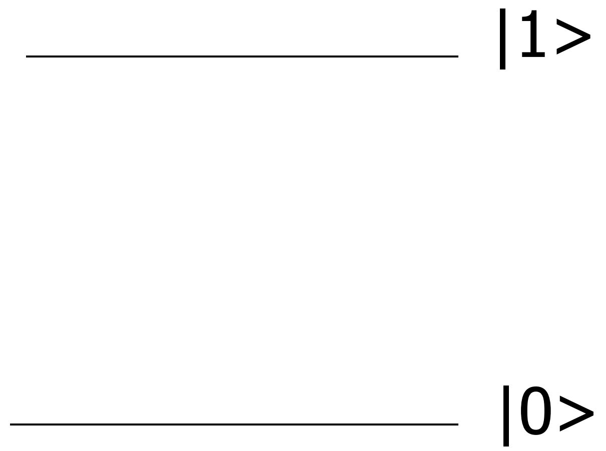
OR		
Input 1	Input B	Output
0	0	0
0	1	1
1	0	1
1	1	1

Classical Algorithm

- We define a Classical Algorithm to be any sequence of such classical operations (usually to do something useful).
- A classical computer is any device that can implement a classical algorithm.

Qubits

- A Quantum Bit (Qubit) is a two-level quantum system.
- We can label the states |0> and |1>.
- In principle, this could be any two-level system.



Qubits

- Unlike a classical bit, which is definitely in either state, the state of a Qubit is in general a mix of |0> and |1>.

$$\left|\psi\right\rangle = c_0\left|0\right\rangle + c_1\left|1\right\rangle$$

- We assume a normalized state:

$$\left|c_0\right|^2 + \left|c_1\right|^2 = 1$$

Qubits

- For convenience, we will use the matrix representation

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Quantum Gate

- A Quantum Logic Gate is an operation that we perform on one or more Qubits that yields another set of Qubits.
- We can represent them as linear operators in the Hilbert space of the system.

Quantum NOT Gate

- As in classical computing, the NOT gate returns a 0 if the input is 1 and a 1 if the input is 0.
- The matrix representation is

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Other Quantum Gates

- Other gates include the Hadamard-Walsh matrix:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- And Phase Flip operation:

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

Multiple Qubits

- Any useful classical computer has more than one bit. Likewise, a Quantum Computer will probably consist of multiple qubits.
- A system of *n* Qubits is called a Quantum Register of length *n*.
- To represent that Qubit 1 has value b_1, Qubit 2 has value b_2, etc., we will use the notation:

$$\left|b_1\right\rangle_1 \left|b_2\right\rangle_2 \cdots \left|b_n\right\rangle_n$$

Multiple Qubits

- For *n* Qubits, the vector representing the state is a *2n* column vector.
- The operations are then *2n* x *2n* matrices.
- For *n* = 2, we use the representations

$$|0\rangle_1|0\rangle_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |0\rangle_1|1\rangle_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |1\rangle_1|0\rangle_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |1\rangle_1|1\rangle_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Quantum CNOT Gate

- An important Quantum Gate for $n = 2$ is the conditional not gate.
- The conditional not gate flips the second bit if and only if the first bit is on.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Input		**Output**	
Qubit 1	Qubit 2	Qubit 1	Qubit 2
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Reversibility and No-Cloning

- In Quantum Computing, we use unitary operations ($U^* U = 1$).
- This ensures that all of the operations that we perform are reversible

Entanglement

- In Quantum Mechanics, it sometimes occurs that a measurement of one particle will effect the state of another particle, even though classically there is no direct interaction. (This is a controversial interpretation).
- When this happens, the state of the two particles is said to be entangled.

Universal Gate Sets

- It would be convenient if there was a small set of operations from which all other operations could be produced.
- That is, a set of operators $\{U_1,\ldots,U_n\}$ such that any other operator W could be written $W = U_iU_j\ldots U_k$.
- Such a set of operators in the context of computation is called a universal gate set.

Classical NAND Gate

- One universal set for Classical Computation consists of only the NAND gate which returns 0 only if the two inputs are 1.

NAND		
Input 1	Input B	Output
0	0	1
0	1	1
1	0	1
1	1	0

$$NOT(P) = NAND(P,P)$$

$$AND(P,Q) = NAND(NAND(P,Q), NAND(P,Q))$$

$$OR(P,Q) = NAND(NAND(P,P), NAND(Q,Q))$$

Quantum Universal Gate Set

- There are a few universal sets in Quantum Computing.
- Two convenient sets:
  - CNOT and single Qubit Gates
  - CNOT, Hadamard-Walsh, and Phase Flips
- Having such a set could greatly simplify implementation and design of Quantum Algorithms.

Physical Implementation

- Any physical implementation of a quantum computer must have the following properties to be practical(DiVincenzo)
  - The number of Qubits can be increased
  - Qubits can be arbitrarily initialized
  - A Universal Gate Set must exist
  - Qubits can be easily read
  - Decoherence time is relatively small

Decoherence

- As the number of Qubits increases, the influence of external environment perturbs the system.
- This causes the states in the computer to change in a way that is completely unintended and is unpredictable, rendering the computer useless.
- This is called decoherence.

Future Prospects

- Currently, research in Quantum Computing is more based on proof-of-principle rather than research into practical applications.
- The infancy of the science is a significant inhibitor. In the future, decoherence may be a serious issue.